REMARKS

The assignee of this application ("Applicant") respectfully requests entry of these preliminary amendments prior to examination. After entry of the amendments claims 4 - 20 will be pending, with claims 1-3 cancelled, and claims 5 - 20 newly added for examination.

Respectfully,

By: _____
Stuart T. F. Huang
Reg. No. 34,184

STEPTOE & JOHNSON LLP
1330 Connecticut Avenue, N.W.
Washington, DC 20036
Tel.: (202) 429-3000
Fax.: (202) 429-3902

VERSION WITH MARKINGS TO SHOW CHANGES

IN THE SPECIFICATION:

Page 1, title:

~~MULTI-STEP DIGITAL SIGNATURE METHOD AND SYSTEM~~ METHOD AND APPARATUS FOR ROAMING USE OF CRYPTOGRAPHIC KEYS

Page 1, first paragraph:

This application is a division of U.S. Patent Application No. 09/161,741, which was a continuation of U.S. Patent Application No.09/869,253, both of which are incorporated herein by reference. ~~This application is a continuation of U.S. Patent Application No. 08/181,859, CRYPTOGRAPHIC SYSTEM WITH KEY ESCROW FEATURE, and U.S. Patent Application Nos. 08/272,203, ENHANCED CRYPTOGRAPHIC SYSTEM AND METHOD WITH KEY ESCROW FEATURE, both of which are incorporated her by reference~~.

Abstract:

A system and method of applying a cryptographic key in the performance of a cryptographic service permits an authorized user of the key to authorize use of the key while the user is physically remote from the key.

~~A multi-step signing system and method uses multiple signing devices to affix a single signature which can be verified using a single public verification key. Each signing device posesses a share of the signature key and affixes a partial signature in response to authorization from a plurality of authorizing agents. In a serial embodiment, after a first partial signature has been affixed, a second signing device exponentiates the first partial signature. In a parallel embodiment, each signing device affixes a partial signature, and the plurality of partial signatures are multiplied together to form the final signature. Security of the system is enhanced by distributing capability to affix signatures among a plurality of signing devices and by distributing authority us affix a partial signature amond a plurality of authorizing agents.~~

IN THE CLAIMS:

Claims 1-3 have been cancelled.

5. A method for remotely invoking the use of a secret cryptographic key share in a process to generate a digital signature where authority to use the secret cryptographic key share lies with an authorizing entity located remotely from the cryptographic key share, the method comprising:

(a) storing the secret cryptographic key share securely in a first computational device at a first location;

(b) communicating, over a communication channel from the authorizing entity at a second location to the computational device at the first location, information that (i) identifies a document to be signed, (ii) identifies the secret cryptographic key share, and (iii) establishes authorization to use the secret cryptographic key share;

(c) at the first location, generating at least a partial result in a cryptographic process to generate the digital signature; and

(d) communicating, from the first location to a location other than the first location, the at lease partial result in the process to generate the digital signature.

6. The method of claim 5 where the step of communicating an authorization to use the secret cryptographic key share includes communicating a hash of the document to be signed to the first location.

7. The method of claim 5 where the step of communicating an authorization to use the secret cryptographic key share includes a step of authenticating the authorizing entity to the first computational device.

8. The method of claim 7 where the step of authenticating the authorizing entity includes a step of signing a communication from the authorizing entity with a signature key associated with the authorizing entity.

9. The method of claim 7 where the step of communicating an authorization to use the secret cryptographic key share includes communicating a certificate identifying the authorizing entity.

10. The method of claim 5 where use of the secret cryptographic key share requires authorization from a plurality of authorizing entities, at least one of which is located remotely from the cryptographic key share.

11. The method of claim 5 where communicating from the authorizing entity at a second location to the computational device at the first location include a step of communicating information in encrypted form.

12. A method for remotely invoking the use of a secret value in a process of providing an electronic service where authority to use the secret value lies with an authorizing entity located remotely from the secret value, the method comprising:

(a) storing the secret value in a first electronic device at a first location;

(b) communicating, over a communication channel from the authorizing entity at a second location to the electronic device at the first location, information identifying (i) the electronic service, (ii) the secret value, and (iii) an authorization to use the secret value;

(c) at the first location, generating an electronic result using the secret value; and

(d) communicating the electronic result from the first location to a location other than the first location.

13. The method of claim 12 where the electronic service is the generation of an electronic signature.

14. The method of claim 13 where communicating an authorization to use the secret value includes communicating, to the first location, a hash of a document to be signed.

15. The method of claim 12 where communicating an authorization to use the secret value includes of authenticating the authorizing entity to the first electronic device.

16. The method of claim 15 where of authenticating the authorizing entity includes signing a communication from the authorizing entity with a signature key associated with the authorizing entity.

17. The method of claim 15 where communicating an authorization to use the secret value includes communicating a certificate identifying the authorizing entity.
value includes communicating a certificate identifying the authorizing entity.

18. The method of claim 1 where use of the secret value requires authorization from a plurality of authorizing entities, at least one of which is located remotely from the secret value.

19. The method of claim 12 where the secret value is a share of a secret key of an asymmetric key pair.

20. The method of claim 12 where communicating from the authorizing entity at a second location to the computational device at the first location include a step of communicating information in encrypted form.